

108TH CONGRESS
1ST SESSION

H. R. 1636

To protect and enhance consumer privacy, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 3, 2003

Mr. STEARNS (for himself, Mr. BOUCHER, Mr. TAUZIN, Mr. TERRY, Mr. BASS, Ms. ESHOO, Mr. WHITFIELD, Mr. GORDON, Mrs. BONO, Mr. MORAN of Virginia, Mr. GILLMOR, Mr. BILIRAKIS, Mr. TOWNS, Mr. DEAL of Georgia, Mr. WELLER, Mr. SHIMKUS, Mr. GREENWOOD, Mr. UPTON, Ms. DEGETTE, Mr. WALDEN of Oregon, Ms. HARMAN, Mr. WELDON of Florida, and Mr. SHADEGG) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To protect and enhance consumer privacy, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Consumer Privacy Pro-
5 tection Act of 2003”.

1 **SEC. 2. TABLE OF CONTENTS.**

2 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.
- Sec. 3. Definitions.

TITLE I—PROTECTION OF INDIVIDUAL PRIVACY IN INTERSTATE
COMMERCE

- Sec. 101. Privacy notices to consumers.
- Sec. 102. Privacy policy statements.
- Sec. 103. Consumer opportunity to limit sale or disclosure of information.
- Sec. 104. Consumer opportunity to limit other information practices.
- Sec. 105. Information security obligations.
- Sec. 106. Self-regulatory programs.
- Sec. 107. Enforcement.
- Sec. 108. No private right of action.
- Sec. 109. Effect on other laws.
- Sec. 110. Effective date.

TITLE II—IDENTITY THEFT PREVENTION AND REMEDIES

- Sec. 201. Facilitating electronic identity theft affidavits.
- Sec. 202. Promoting use of common identity theft affidavit.
- Sec. 203. Timely resolution of identity theft disputes.
- Sec. 204. Improvements to consumer clearinghouse.
- Sec. 205. Improved identity theft data.
- Sec. 206. Change of address protections.
- Sec. 207. Effective date.

TITLE III—INTERNATIONAL PROVISIONS

- Sec. 301. Study by Comptroller General.
- Sec. 302. Remediation of discriminatory impact by Secretary of Commerce.
- Sec. 303. Effect of nonremediation.
- Sec. 304. Harmonization of international privacy laws, regulations, and agreements.

3 **SEC. 3. DEFINITIONS.**

4 In this Act:

- 5 (1) The term “Commission” means the Federal
- 6 Trade Commission.
- 7 (2) The term “consumer” means an individual
- 8 acting in the individual’s personal, family, or house-
- 9 hold capacity.

1 (3)(A) The term “data collection organization”
2 means an entity (or an agent or affiliate of the enti-
3 ty) that collects (by any means, through any me-
4 dium), sells, discloses for consideration, or uses per-
5 sonally identifiable information of the consumer.

6 (B) Such term does not include—

7 (i) a governmental agency;

8 (ii) a not-for-profit entity, to the ex-
9 tent that personally identifiable informa-
10 tion is not used for a commercial purpose;

11 (iii) an entity that—

12 (I) has annual gross revenue
13 under \$1,000,000 (based on the value
14 of such amount in fiscal year 2000,
15 adjusted for current dollars);

16 (II) has fewer than 25 employees;

17 (III) collects or uses personally
18 identifiable information from fewer
19 than 1,000 consumers for a purpose
20 unrelated to a transaction with the
21 consumer;

22 (IV) does not process personally
23 identifiable information of consumers;
24 and

1 (V) does not sell or disclose for
2 consideration such information to an-
3 other person;

4 (iv) a provider of professional services,
5 or any affiliate thereof, to the extent that
6 such provider is obligated by rules of pro-
7 fessional ethics, or by applicable law or
8 regulation, not to voluntarily disclose con-
9 fidential client information without the
10 consent of the client; or

11 (v) a data processing outsourcing enti-
12 ty.

13 (4)(A) The term “personally identifiable infor-
14 mation”, with respect to a data collection organiza-
15 tion means individually identifiable information re-
16 lating to a living individual who can be identified
17 from that information.

18 (B) Such term includes—

19 (i) first and last name, whether given
20 at birth or adoption, assumed, or legally
21 changed;

22 (ii) home or other physical address in-
23 cluding street name and name of a city or
24 town;

25 (iii) electronic mail address;

1 (iv) telephone number;

2 (v) social security number; or

3 (vi) any other unique identifying in-
4 formation that a data collector and proc-
5 essor collects and combines with any infor-
6 mation described in the preceding subpara-
7 graphs of this paragraph.

8 (C) Such term does not include—

9 (i) anonymous or aggregate data, or
10 any other information that does not iden-
11 tify a unique living individual;

12 (ii) information about a consumer in-
13 ferred from data maintained about a con-
14 sumer; or

15 (iii) information about a consumer ob-
16 tained from a public record.

17 (5) The term “affiliate” means any company
18 that controls, is controlled by, or is under common
19 control with another company.

20 (6) The term “information-sharing affiliate”
21 means any affiliate that is under common control
22 with a data collection organization, and is contrac-
23 tually obligated to comply with the practices enu-
24 merated under the privacy policy statement of the
25 organization required under section 102.

1 (7) The term “data processing outsourcing enti-
2 ty” means, with respect to a data collection organi-
3 zation, a non-affiliated entity that—

4 (A) provides information technology proc-
5 essing, Web hosting, or telecommunications
6 services to the data collection organization;

7 (B) is contractually obligated to comply
8 with security controls specified by the data col-
9 lection organization; and

10 (C) has no right to use the data collection
11 organization’s personally identifiable informa-
12 tion other than for performing data processing
13 outsourcing services for the data collection or-
14 ganization or as required by law.

15 (8) The term “process”, with respect to person-
16 ally identifiable information, means any value-added
17 activity performed on data by automated means.

18 (9) The term “transaction” means an inter-
19 action between a consumer and a data collection or-
20 ganization resulting in—

21 (A) any use of information that is nec-
22 essary to complete the interaction in the course
23 of which information is collected, or to maintain
24 the provisioning of a good or service requested
25 by the consumer, including use—

1 (i) to approve, guarantee, process, ad-
2 minister, complete, enforce, provide, or
3 market a product, service, account, benefit,
4 transaction, or payment method that is re-
5 quested or approved by the consumer; or

6 (ii) to deliver goods, services, funds,
7 or other consideration to, or on behalf of,
8 the consumer;

9 (B) any disclosure of information that is
10 necessary for the consumer to enforce any right
11 of the consumer;

12 (C) any disclosure of information that is
13 required by law or by a court order; and

14 (D) any use of information to verify per-
15 sonally identifiable information by the con-
16 sumer, evaluate, detect, or reduce the risk of
17 fraud or other criminal activity, or other risk-
18 management activities.

19 (10) The term “display” means intentionally
20 communicating or otherwise making available (on
21 the Internet or in any other manner) to another per-
22 son.

23 (11) The term “public record” means any item,
24 collection, or grouping of information about an indi-
25 vidual that is maintained by a Federal, State, or

1 local government entity and that is made available
2 to the public.

3 (12) The term “purchase” means providing, di-
4 rectly or indirectly, anything of value in exchange
5 for a good or service.

6 (13) The term “State” includes the several
7 States, the District of Columbia, the Commonwealth
8 of Puerto Rico, the Commonwealth of the Northern
9 Mariana Islands, American Samoa, Guam, the Vir-
10 gin Islands, the Freely Associated States, and any
11 other territory or possession of the United States.

12 **TITLE I—PROTECTION OF INDIVIDUAL PRIVACY IN INTER-**
13 **STATE COMMERCE**
14

15 **SEC. 101. PRIVACY NOTICES TO CONSUMERS.**

16 (a) NOTICE REQUIRED.—A data collection organiza-
17 tion shall provide to a consumer a notice containing the
18 information required under subsection (b) as follows:

19 (1) Upon the first instance of collection from
20 the consumer of personally identifiable information,
21 that may be used for a purpose unrelated to the
22 transaction, by a data collection organization, the or-
23 ganization shall provide the notice at the time per-
24 sonally identifiable information is collected.

1 (2) Upon a material change in the organiza-
2 tion's privacy policy under section 102(a), the orga-
3 nization shall provide the notice, not later than the
4 first time after such change in policy that the orga-
5 nization seeks to collect, sell, disclose for consider-
6 ation, or use personally identifiable information to
7 the extent practicable, to each consumer from whom
8 the organization has collected such information.

9 (b) FORM AND CONTENTS OF NOTICE.—A notice re-
10 quired under subsection (a) shall be provided in a clear
11 and conspicuous manner, be prominently displayed or ex-
12 plicitly stated to the consumer, and contain the following
13 information:

14 (1) A statement that the personal information
15 collected by the data collection organization may be
16 used or disclosed for purposes or transactions unre-
17 lated to that for which it was collected, as described
18 in the organization's privacy statement.

19 (2) A description of the manner in which the
20 consumer may obtain a privacy policy statement that
21 meets the requirements of section 102, which may
22 include providing the consumer with an Internet
23 website, a hyperlink to such a website, or a toll-free
24 telephone number from which such a statement may
25 be obtained. If the notice required under subsection

1 (a) is provided to the consumer by means of an
2 Internet website, one manner in which the consumer
3 may obtain the privacy policy statement must be by
4 means of an Internet website.

5 (3) If the notice is required under subsection
6 (a)(2), a statement that there has been a material
7 change in the organization's privacy policy.

8 **SEC. 102. PRIVACY POLICY STATEMENTS.**

9 (a) **PRIVACY POLICY.**—A data collection organization
10 shall establish a privacy policy with respect to the collec-
11 tion, sale, disclosure for consideration, dissemination, use,
12 and security of the personally identifiable information of
13 consumers, the principal elements of which shall be em-
14 bodied in a privacy policy statement (or statements) that
15 meets the requirements of subsection (b).

16 (b) **STATEMENT.**—The statement (or statements) re-
17 quired under subsection (a) shall meet the following re-
18 quirements:

19 (1) The statement must be brief, concise, clear,
20 and conspicuous and written in plain language.

21 (2) The statement must be accessible to all con-
22 sumers of the data collection organization (regard-
23 less of the means by which a consumer conducts a
24 transaction with the organization)—

25 (A) at no charge to the consumer; and

1 (B) at the time the data collection organi-
2 zation first collects personally identifiable infor-
3 mation about the consumer that may be used
4 for a purpose unrelated to a transaction with
5 the consumer and subsequently.

6 (3) The statement must disclose only the fol-
7 lowing:

8 (A) The identity of each data collection or-
9 ganization, or a description of each class or
10 type of data collection organization, that may
11 collect or use the information.

12 (B) The types of information that may be
13 collected or used.

14 (C) How the information may be used.

15 (D) Whether the consumer is required to
16 provide the information in order to do business
17 with the data collection organization.

18 (E) The extent to which the information is
19 subject to sale or disclosure for consideration to
20 a data collection organization that is not an in-
21 formation-sharing affiliate of the data collection
22 organization providing the statement, includ-
23 ing—

1 (i) a clear and prominent statement of
2 the fact that the information is subject to
3 such sale or disclosure for consideration;

4 (ii) a description of each class or type
5 of data collection organization to which the
6 information may be sold or disclosed for
7 consideration;

8 (iii) to the extent practicable, the pur-
9 pose for which the information may be
10 used; and

11 (iv) the types of information that may
12 be sold or disclosed for consideration.

13 (F) Whether the information security prac-
14 tices of the data collection organization meet
15 the security requirements of section 105 in
16 order to prevent unauthorized disclosure or re-
17 lease of personally identifiable information.

18 (c) COMMISSION FACILITATION.—The Commission
19 shall take actions (including conducting industry-wide
20 workshops) to facilitate the development of harmonized,
21 universal wording or logo-based graphics in order to con-
22 vey the contents of privacy policy statements required
23 under this section.

1 **SEC. 103. CONSUMER OPPORTUNITY TO LIMIT SALE OR DIS-**
2 **CLOSURE OF INFORMATION.**

3 (a) PRECLUSION OF SALE OR DISCLOSURE.—

4 (1) REQUIREMENT.—A data collection organi-
5 zation shall provide to the consumer, without charge,
6 the opportunity to preclude any sale or disclosure for
7 consideration of the consumer's personally identifi-
8 able information, provided in a particular data col-
9 lection, that may be used for a purpose other than
10 a transaction with the consumer, to any data collec-
11 tion organization that is not an information-sharing
12 affiliate of the data collection organization providing
13 such opportunity

14 (2) DURATION.—A preclusion on sale or disclo-
15 sure for consideration of information established by
16 a consumer under this subsection shall remain in ef-
17 fect for 5 years or until the consumer indicates oth-
18 erwise, whichever occurs sooner. A data collection
19 organization may not seek reconsideration of a con-
20 sumer's preclusion of such sale or disclosure until at
21 least 1 year after such preclusion has been imposed
22 by the consumer.

23 (b) PERMISSION FOR SALE OR DISCLOSURE.—A data
24 collection organization may provide the consumer an op-
25 portunity to permit the sale or disclosure described in sub-
26 section (a)(1) in exchange for a benefit to the consumer.

1 (c) ACCESSIBILITY.—The opportunity to preclude (or
 2 if offered, to permit) the sale or disclosure for consider-
 3 ation of information under this section must be both easy
 4 to access and use, and the notice of the opportunity to
 5 preclude must be clear and conspicuous..

6 **SEC. 104. CONSUMER OPPORTUNITY TO LIMIT OTHER IN-**
 7 **FORMATION PRACTICES.**

8 If a data collection organization provides to a con-
 9 sumer the opportunity to limit other practices of the data
 10 collection organization with respect to a particular collec-
 11 tion or use of personally identifiable information regarding
 12 the consumer, other than that required by section 103—

13 (1) a notice and description of such opportunity
 14 must appear in the privacy statement;

15 (2) such opportunity must be easy to access
 16 and to use; and

17 (3) any limitation exercised by the consumer
 18 pursuant to such opportunity shall remain in effect,
 19 unless—

20 (A) the limitation is withdrawn by the con-
 21 sumer; or

22 (B) the data collection organization pro-
 23 vides the consumer at least 30 days notice be-
 24 fore materially changing the limitation or termi-
 25 nating its compliance with the limitation.

1 **SEC. 105. INFORMATION SECURITY OBLIGATIONS.**

2 (a) INFORMATION SECURITY POLICY.—

3 (1) IMPLEMENTATION.—A data collection orga-
4 nization shall prepare, revise as necessary, and im-
5 plement an information security policy that is appli-
6 cable to the information security practices and treat-
7 ment of personally identifiable information main-
8 tained by the data collection organization, that is de-
9 signed to prevent the unauthorized disclosure or re-
10 lease of such information.

11 (2) MANAGEMENT APPROVAL.—An information
12 security policy created pursuant to paragraph (1)
13 shall be considered and approved by the senior man-
14 agement officials of the data collection organization.

15 (3) CONTENTS.—An information security policy
16 required under paragraph (1) shall include—

17 (A) a process for taking corrective action
18 pursuant to subsection (b); and

19 (B) identifying an officer of the data col-
20 lection organization as the point of contact with
21 responsibility for information security issues for
22 the organization.

23 (b) CORRECTIVE ACTIONS.—

24 (1) INFORMATION SECURITY ADVISORIES AND
25 ACTION.—Except as provided in paragraph (2), upon
26 the issuance of an information security advisory (as

1 such term is defined in subsection (d)), a data col-
2 lection organization shall, within a reasonable period
3 of time after the issuance of such advisory and pur-
4 suant to its information security policy, take appro-
5 priate action reasonably necessary to mitigate
6 against any vulnerability identified in such advisory,
7 including implementing any changes to its security
8 practices and the architecture, installation, or imple-
9 mentation of its network or operating software (in-
10 cluding corrective patches) in response to such advi-
11 sory.

12 (2) EXCEPTIONS.—A data collection organiza-
13 tion shall not be required to take the action specified
14 in an information security advisory under paragraph
15 (1) if such organization can, in good faith, show
16 that—

17 (A) the corrective action required would
18 cause harm to, or weaken, the organization's
19 existing information security for personally
20 identifiable information or the procedures or
21 systems of the organization;

22 (B) the organization takes, or has taken,
23 other appropriate steps or corrective action to
24 mitigate the vulnerabilities and exposure risks

1 identified in the information security advisory;
2 or

3 (C) the specified corrective action is not
4 necessary.

5 (c) EFFECT OF RELEASE OF PERSONALLY IDENTIFI-
6 ABLE INFORMATION.—If the security of a data collection
7 organization has been compromised, resulting in the unau-
8 thorized release of a consumer’s personally identifiable in-
9 formation, the data collection organization shall be pre-
10 sumed to be in violation of this section if such organization
11 has failed to respond to an information security advisory
12 in accordance with subsection (b)(1).

13 (d) DEFINITION.—As used in this section, the term
14 “information security advisory” means an information se-
15 curity advisory issued by the Federal Computer Incident
16 Response Center of the Department of Homeland Secu-
17 rity, or its successor agency.

18 **SEC. 106. SELF-REGULATORY PROGRAMS.**

19 (a) SELF-REGULATORY PROGRAM.—

20 (1) PRESUMPTION OF COMPLIANCE.—The Com-
21 mission shall presume that a data collection organi-
22 zation is in compliance with the provisions of sec-
23 tions 101 through 105 if that organization—

24 (A) participates in a self-regulatory pro-
25 gram approved under subsection (b); and

1 (B) has been determined by a self-regu-
2 latory program to be in compliance with the
3 guidelines, procedures, requirements, and re-
4 strictions of the program (including a remedial
5 process under subsection (c)(7)).

6 (2) EFFECT OF WILLFUL NONCOMPLIANCE.—A
7 data collection organization that participates in a
8 self-regulatory program under this section shall not
9 be liable for a civil penalty arising out of a violation
10 of any provision of sections 101 through 105 unless
11 such violation results from willful noncompliance
12 with the guidelines, procedures, requirements, or re-
13 strictions of the program.

14 (b) APPROVAL BY COMMISSION.—

15 (1) APPROVAL.—The Commission shall, within
16 90 days after submission of an application for ap-
17 proval of a self-regulatory program under this sec-
18 tion (or of a material change in a program pre-
19 viously approved by the Commission), approve such
20 program (or change) if the Commission finds that
21 the program (or change) complies with the require-
22 ments of subsection (c).

23 (2) FORM OF APPLICATION.—The Commission
24 shall accept an application for approval under para-

1 graph (1) in any reasonable form the applicant may
2 submit.

3 (3) DURATION UNTIL RENEWAL.—A self-regu-
4 latory program approved by the Commission under
5 paragraph (1) shall be approved for a period of 5
6 years.

7 (4) REVOCATION OF APPROVAL.—The Commis-
8 sion may, after notice and opportunity for a hearing,
9 revoke approval granted under paragraph (1), if the
10 Commission finds that a self-regulatory program
11 fails to meet the requirements of subsection (c).

12 (5) JUDICIAL REVIEW.—Any order by the Com-
13 mission denying approval of a self-regulatory pro-
14 gram shall be subject to judicial review, as provided
15 in section 706 of title 5, United States Code.

16 (c) REQUIREMENTS OF SELF-REGULATORY PRO-
17 GRAM.—A self-regulatory program complies with the re-
18 quirements of this subsection if the program provides each
19 of the following:

20 (1) Guidelines and procedures requiring a pro-
21 gram participant to provide substantially equivalent
22 or greater protections for consumers and their per-
23 sonally identifiable information as are provided
24 under sections 101 through 105.

1 (2) Procedures and requirements to provide
2 for—

3 (A) an initial review of a participant's pri-
4 vacy statement and privacy policy, and subse-
5 quent review whenever such statement or policy
6 is substantively changed, to determine whether
7 the participant complies with the self-regulatory
8 program's guidelines;

9 (B) an initial self-review and self-certifi-
10 cation of a participant's privacy policy and
11 practices to ensure compliance with the guide-
12 lines, procedures, requirements, and restrictions
13 of the program established under this sub-
14 section;

15 (C) subsequent periodic self-reviews and
16 self-certifications, which shall occur at least an-
17 nually, of the participant's privacy policy and
18 practices to ensure continued compliance with
19 such guidelines, procedures, requirements, and
20 restrictions;

21 (D) submission of self-reviews and self-cer-
22 tifications under this paragraph to any adminis-
23 trator of the program; and

24 (E) random compliance testing of partici-
25 pants, which may concentrate on selected com-

1 compliance issues, if the self-regulatory program
2 conducts—

3 (i) a random compliance test with re-
4 spect to each participant not less fre-
5 quently than every 3 years;

6 (ii) a full compliance test in any case
7 where non-compliance with any of the se-
8 lected compliance issues is identified; and

9 (iii) full compliance tests of partici-
10 pants with a high number of complaints
11 against them.

12 (3) Procedures and requirements that ensure
13 that a program participant provides a process for re-
14 solving disputes with consumers relating to the pri-
15 vacy policy and practices of the participant. Such
16 dispute resolution process—

17 (A) must be available without charge to a
18 consumer;

19 (B) must be available at a cost to the par-
20 ticipant that is reasonable and does not discour-
21 age participation by the participant in such
22 process;

23 (C) must ensure that consumers are in-
24 formed of how to utilize the process;

1 (D) may include, as one choice among oth-
2 ers, binding arbitration; and

3 (E)(i) must be completed within 60 days
4 after submission of the dispute by the con-
5 sumer; or

6 (ii) must be completed within 90 days after
7 submission of the dispute by the consumer, if
8 the participant—

9 (I) determines that additional
10 time is required to obtain information
11 to make an informed decision with re-
12 spect to the dispute; and

13 (II) notifies the consumer and
14 the self-regulatory program that such
15 additional time is required.

16 (4) Provisions for the use by participants in the
17 program of a means (including the use of a seal) to
18 represent the participant's participation in the pro-
19 gram.

20 (5) With respect to any nonvoluntary suspen-
21 sion or termination of participation in the program
22 because of the participant's failure to comply with
23 the program, procedures or requirements to provide
24 for the following:

1 (A) Publication of notice and the reasons
2 for any such suspension or termination, except
3 that no personally identifiable information re-
4 lated to such suspension or termination may be
5 published.

6 (B) Notice to the Commission of any such
7 termination.

8 (6) Requirements and restrictions that assure
9 independence with respect to program eligibility,
10 compliance, and dispute resolution mechanisms and
11 decisions from improper interference by management
12 or ownership of the self-regulatory program partici-
13 pant.

14 (7) A process for a noncompliant participant to
15 take timely remedial action in order to come back
16 into compliance with the program before suspension
17 or termination of participation in the program.

18 (d) CONSUMER DISPUTE RESOLUTION.—

19 (1) SELF-REGULATORY DISPUTE PROCESS.—If
20 a consumer has a dispute with a participant in a
21 self-regulatory program under this section or under
22 section 5 of the Federal Trade Commission Act (15
23 U.S.C. 45) to the extent that such dispute pertains
24 to the entity's privacy policy or practices required
25 for participation in the self-regulatory program, the

1 consumer shall initially seek resolution through the
2 participant's dispute resolution process (established
3 in accordance with subsection (c)(3)). The Commis-
4 sion shall promptly refer to the participant involved
5 any dispute submitted to the Commission for which
6 resolution has not been initially sought through such
7 process.

8 (2) RESOLUTION BY COMMISSION.—A consumer
9 may submit to the Commission for resolution a dis-
10 pute with a participant in a self-regulatory program
11 under this section, if the following requirements are
12 met:

13 (A) The dispute was initially submitted
14 under paragraph (1) for resolution through the
15 participant's dispute resolution process.

16 (B) The dispute submitted under para-
17 graph (1) is not resolved—

18 (i) within 60 days after submission of
19 the dispute by the consumer; or

20 (ii) to the satisfaction of the con-
21 sumer.

22 (C) Notice of the facts of the dispute is
23 submitted to the Commission not later than 30
24 days after the date on which the consumer is

1 notified of the resolution through the partici-
2 pant's dispute resolution process.

3 (D) The consumer has not voluntarily ac-
4 cepted a resolution of the dispute under para-
5 graph (1).

6 (E) The dispute was not resolved through
7 binding arbitration.

8 (3) LIMITATION.—Nothing in this Act shall
9 prevent the Commission from investigating compli-
10 ance with this Act by a participant in a self-regu-
11 latory organization based upon a complaint from an
12 individual or organization other than a consumer
13 with a dispute with such participant, or on its own
14 initiative, except that prior to instituting any such
15 investigation the Commission shall afford the self-
16 regulatory organization a reasonable opportunity to
17 invoke its own remedial procedures and assure com-
18 pliance by the participant.

19 (4) CLEAR AND CONVINCING EVIDENCE.—The
20 presumption established by paragraph (1) of sub-
21 section (a) may be overcome by clear and convincing
22 evidence of non-compliance.

23 (e) NONRELEASE OF CERTAIN INFORMATION.—The
24 Commission may not compel a participant in a self-regu-
25 latory program approved under subsection (b) (or an ad-

1 administrator of such a program) to provide proprietary in-
2 formation or personally identifiable information of con-
3 sumers to the Commission unless the Commission provides
4 assurances that such information will not be released to
5 the public.

6 (f) MISREPRESENTATION OF SELF-REGULATORY
7 PROGRAM PARTICIPATION.—It is unlawful for a data col-
8 lection organization to misrepresent that it is a participant
9 in a self-regulatory program (including through any mech-
10 anism provided under subsection (c)(4)) when such orga-
11 nization is not, in fact, such a participant.

12 (g) EXEMPTED ENTITY PARTICIPATION.—An entity
13 that is not a data collection organization and that volun-
14 tarily participates in a self-regulatory program under this
15 section shall enjoy the rights and benefits provided under
16 this section in any action or investigation under section
17 5 of the Federal Trade Commission Act (15 U.S.C. 45)
18 to the extent that such action or investigation pertains to
19 the entity’s privacy policy or practices required for partici-
20 pation in the self-regulatory program.

21 **SEC. 107. ENFORCEMENT.**

22 (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A
23 violation of any provision of this title by a data collection
24 organization is an unfair or deceptive act or practice un-
25 lawful under section 5(a)(1) of the Federal Trade Com-

1 mission Act (15 U.S.C. 45(a)(1)), except that the amount
2 of any civil penalty under such Act shall be doubled for
3 a violation of this title, but may not exceed \$500,000 for
4 all related violations by a single violator (without respect
5 to the number of consumers affected or the duration of
6 the related violations).

7 (b) GUIDELINES AND OPINIONS.—In order to assist
8 in compliance with this title, the Federal Trade Commis-
9 sion may promulgate regulations and interpretive rules
10 under section 18 of the Federal Trade Commission Act
11 (15 U.S.C. 57a), with respect to specific types of acts or
12 practices that would, or would not, comply with this title.

13 **SEC. 108. NO PRIVATE RIGHT OF ACTION.**

14 This title may not be considered or construed to pro-
15 vide any private right of action. No private civil action
16 relating to any act or practice governed under this title
17 may be commenced or maintained in any State court or
18 under State law (including a pendent State claim to an
19 action under Federal law).

20 **SEC. 109. EFFECT ON OTHER LAWS.**

21 (a) QUALIFIED EXEMPTION FOR COMPLIANCE WITH
22 OTHER FEDERAL PRIVACY LAWS.—To the extent that
23 personally identifiable information protected under this
24 title is also protected under a provision of Federal privacy
25 law described in subsection (c), a data collection organiza-

tion that complies with the relevant provision of such other Federal privacy law shall be deemed to have complied with the corresponding provision of this title.

(b) PROTECTION OF OTHER FEDERAL PRIVACY LAWS.—Nothing in this title may be construed to modify, limit, or supersede the operation of the Federal privacy laws described in subsection (c) or the provision of information permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(c) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—The provisions of law to which subsections (a) and (b) apply are the following:

(1) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974).

(2) The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.).

(3) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(4) The Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.).

(5) The Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(6) Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 et seq.).

1 (7) The Electronic Communications Privacy Act
2 of 1986 (Public Law 99–508).

3 (8) The Driver’s Privacy Protection Act of
4 1994 (18 U.S.C. 2721 et seq.).

5 (9) The Family Educational Rights and Privacy
6 Act of 1974 (20 U.S.C. 1221 note, 1232g).

7 (10) Section 445 of the General Education Pro-
8 visions Act (20 U.S.C. 1232h).

9 (11) The Privacy Protection Act of 1980 (42
10 U.S.C. 2000aa et seq.).

11 (12) Section 222 of the Communications Act of
12 1934 (47 U.S.C. 222) relating to the Customer Pro-
13 prietary Network Information.

14 (13) The Cable Communications Policy Act of
15 1984 (47 U.S.C. 521 et seq.).

16 (14) The Communications Assistance for Law
17 Enforcement Act (47 U.S.C. 1001 et seq.).

18 (15) The Video Privacy Protection Act of 1988
19 (Public Law 100–618).

20 (16) The Telephone Consumer Protection Act
21 of 1991 (Public Law 102–243).

22 (17) The Health Insurance Portability and Ac-
23 countability Act of 1996 (Public Law 104–191), as
24 it relates to an entity described in section 1172(a)
25 of the Social Security Act (42 U.S.C. 1320d-1(a)) or

1 to activities regulated under section 1173 of such
 2 Act (42 U.S.C. 1320d-2).

3 (d) PREEMPTION OF STATE PRIVACY LAWS.—This
 4 title preempts any statutory law, common law, rule, or
 5 regulation of a State, or a political subdivision of a State,
 6 to the extent such law, rule, or regulation relates to or
 7 affects the collection, use, sale, disclosure, retention, or
 8 dissemination of personally identifiable information in
 9 commerce. No State, or political subdivision of a State,
 10 may take any action to enforce this title.

11 **SEC. 110. EFFECTIVE DATE.**

12 This title shall apply with respect to personally identi-
 13 fiable information collected on or after the date that is
 14 1 year after the date of enactment of this Act.

15 **TITLE II—IDENTITY THEFT**
 16 **PREVENTION AND REMEDIES**

17 **SEC. 201. FACILITATING ELECTRONIC IDENTITY THEFT AF-**
 18 **FIDAVITS.**

19 The Commission shall take such action as necessary
 20 to permit (including by electronic means) consumers that
 21 have a reasonable belief that they are a victim of identity
 22 theft—

23 (1) to enter required consumer information in
 24 the commission-developed document entitled “Iden-
 25 tity Theft Affidavit”; and

1 (2) to submit completed forms and other sup-
2 plemental information to the Commission and other
3 entities.

4 **SEC. 202. PROMOTING USE OF COMMON IDENTITY THEFT**
5 **AFFIDAVIT.**

6 The Commission shall take such action as necessary
7 to solicit the acceptance and acknowledgement of stand-
8 ardized Identity Theft Affidavit by entities that receive
9 disputes regarding the unauthorized use of accounts of
10 such entities from consumers that have reason to believe
11 that they are victims of identity theft.

12 **SEC. 203. TIMELY RESOLUTION OF IDENTITY THEFT DIS-**
13 **PUTES.**

14 The Commission shall require entities that receive
15 disputes regarding the unauthorized use of accounts of
16 such entities from consumers that have reason to believe
17 that they are victims of identity theft to conduct any nec-
18 essary investigation and decide an outcome of a claim
19 within 90 days from the date on which all necessary infor-
20 mation to investigate the claim has been submitted to the
21 entity.

22 **SEC. 204. IMPROVEMENTS TO CONSUMER CLEARING-**
23 **HOUSE.**

24 The Commission shall utilize the Identity Theft
25 Clearinghouse to permit consumers that have a reasonable

1 belief that they are victims of identity theft to submit any
2 information relevant to such identity theft to the Clearing-
3 house (including by means of an Identity Theft Affidavit),
4 so that such information may be transmitted by the Clear-
5 inghouse to appropriate entities for necessary protective
6 action and to mitigate losses resulting from such identity
7 theft.

8 **SEC. 205. IMPROVED IDENTITY THEFT DATA.**

9 (a) IN GENERAL.—The Commission shall—

10 (1) establish a process to contact, not less than
11 annually, public and private entities that receive and
12 process complaints from consumers that have a rea-
13 sonable belief that they are victims of identity theft;
14 and

15 (2) obtain accurate data on the incidences and
16 nature of complaints from such entities.

17 (b) INCLUSION IN DATABASE.—Such information
18 shall be made part of the Commission’s Identity Theft
19 Clearinghouse database.

20 **SEC. 206. CHANGE OF ADDRESS PROTECTIONS.**

21 The Commission shall require appropriate entities to
22 take reasonable steps to verify the accuracy of a con-
23 sumer’s address, including by confirming a consumer’s
24 change of address by sending a confirmation of such
25 change to the old and the new address of the consumer.

1 **SEC. 207. EFFECTIVE DATE.**

2 This title shall take effect 180 days after the date
3 of enactment of this Act.

4 **TITLE III—INTERNATIONAL**
5 **PROVISIONS**

6 **SEC. 301. STUDY BY COMPTROLLER GENERAL.**

7 The Comptroller General of the United States shall
8 conduct a study and issue a report analyzing the impact
9 on the interstate and foreign commerce of the United
10 States of information privacy laws, regulations, or agree-
11 ments enacted, promulgated, or adopted by other nations,
12 including regional or international agreements between
13 nations, and whether the enforcement mechanisms or pro-
14 cedures of those laws, regulations, or agreements result
15 in discriminatory treatment of United States entities. The
16 first report under this section shall be issued not later
17 than 120 days after the date of enactment of this Act and
18 subsequent reports shall be issued every 3 years there-
19 after.

20 **SEC. 302. REMEDIATION OF DISCRIMINATORY IMPACT BY**
21 **SECRETARY OF COMMERCE.**

22 If the Comptroller General of the United States finds,
23 in the study and report under section 301, that such infor-
24 mation privacy laws, regulations, or agreements substan-
25 tially impede interstate and foreign commerce of the
26 United States and that the enforcement mechanisms or

1 procedures of the information privacy laws, regulations,
2 or agreements described in such subsection result in dis-
3 criminatory treatment of United States entities, the Sec-
4 retary of Commerce shall, to the extent permitted by law
5 take all steps necessary to mitigate against such discrimi-
6 natory impact within 180 days after the report making
7 such findings is issued.

8 **SEC. 303. EFFECT OF NONREMEDATION.**

9 (a) RECOMMENDATIONS.—If by the end of the 180-
10 day period described in section 302, the Secretary of Com-
11 merce has not attained complete relief from the discrimi-
12 natory impact described in such subsection, the Secretary
13 shall report to the Congress and the President rec-
14 ommendations on action to relieve any such remaining dis-
15 criminatory impact.

16 (b) FEDERAL AGENCY ACTION AFTER CONSIDER-
17 ATION BY CONGRESS.—During the period after the Sec-
18 retary reports recommendations under subsection (a) for
19 mitigation of discriminatory impact and before the Con-
20 gress acts with respect to such recommendations, no offi-
21 cer or employee of any Federal agency may take or con-
22 tinue any action to enjoin, or impose any penalty on, a
23 United States entity, or a citizen or legal resident of the
24 United States, for the purpose of fulfilling an international
25 obligation of the United States under an international pri-

1 vacy agreement (other than such an obligation under a
2 ratified treaty) that resulted in such discriminatory im-
3 pact.

4 **SEC. 304. HARMONIZATION OF INTERNATIONAL PRIVACY**
5 **LAWS, REGULATIONS, AND AGREEMENTS.**

6 Beginning on the date of enactment of this Act, the
7 Secretary of Commerce shall provide notice of the provi-
8 sions of this Act to other nations, individually, or as mem-
9 bers of international organizations or unions that have en-
10 acted, promulgated, or adopted information privacy laws,
11 regulations, or agreements, and shall seek recognition of
12 this Act by such nations, organizations, or unions. The
13 Secretary shall seek the harmonization of this Act with
14 such information privacy laws, regulations, or agreements,
15 to the extent such harmonization is necessary for the ad-
16 vancement of transnational commerce, including electronic
17 commerce.

